IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 3:17-CR-086
	)	
ADAM C. MARKS,	)	Count One: 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(iii) (Unauthorized Access to a Protected Computer) BRH MJS
	)	
Defendant.	)	
	)	Count Two: 18 U.S.C. § 1030(a)(5)(A) (Knowingly and Intentionally Damaging a Protected Computer)

July 2017 Term – at Richmond, Virginia

INDICTMENT

The Grand Jury charges that:

Introduction

At all times material to this indictment:

1. Estes Forwarding Worldwide (EFW) is a global shipping company headquartered in Richmond, Virginia, with regional offices in multiple states. During the period set forth in this indictment, EFW conducted business in the Eastern District of Virginia and elsewhere.

2. Salesforce.com is a cloud computing company headquartered in San Francisco, California. Salesforce.com offers a web-based platform called Salesforce, which numerous companies, organizations and educational institutions use as a customer relationship management (CRM) tool. Salesforce.com maintains its

Salesforce CRM platform on servers used in interstate and foreign commerce, which customers would access through a password-protected portal. Customers of Salesforce.com, like EFW, would access their respective "instance" of the Salesforce CRM tool by using one or more email addresses, along with the appropriate password(s), assigned to that company's Salesforce account.

3. The defendant, ADAM C. MARKS, worked at EFW as an administrator for their Salesforce account for a period of approximately two and a half years, which ended on December 6, 2013. On that date, MARKS left employment with EFW to pursue a Salesforce administrator position with another employer.

4. As part of his exit process from EFW, MARKS's authorization to access EFW's Salesforce portal and authority to access EFW-owned networks was terminated on December 6, 2013.

5. On December 6, 2013, MARKS logged on to the Salesforce platform and changed the e-mail address associated with his EFW's Salesforce user profile of "amarks@efwnow.com," from adam.marks@efwnow.com to a personal Gmail account.

6. On December 8, 2013, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce portal and account, and changed password policies for EFW's Salesforce accounts.

7. On December 9, 2013, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce portal and account, and using the data administrator user profile, *i.e.*,

"data.admin@efwnow.com," unfroze his previously frozen Salesforce user profile of "amarks@efwnow.com."

8. On December 9, 2013, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce account, and created a user profile named "informatica_secure_agent@efwnow.com," which had administrator privileges.

9. On December 18, 2013, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce account, logged into the "data.admin@efwnow.com" user profile and emptied items from EFW's Salesforce Recycle Bin.

10. On January 8, 2014, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce account, and changed the password to the "data.admin@efwnow.com" user profile.

11. On January 28, 2014, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce account, and used the "informatica_secure_agent@efwnow.com" user profile to freeze EFW's Salesforce system administrators' accounts.

12. On January 28, 2014, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce account, reactivated the "data.admin@efwnow.com" user profile and changed the lead owner of EFW's Salesforce account to the "data.admin@efwnow.com" user profile.

13. On January 28, 2014, MARKS intentionally accessed without authorization a protected computer, to wit, the Salesforce platform via EFW's Salesforce account, and using the reactivated "data.admin@efwnow.com" user profile changed EFW's Salesforce system administrator accounts from system administrator privileges to standard user privileges.

COUNT ONE
(Unauthorized Access to a Protected Computer)

14. The Grand Jury realleges and incorporates the allegations of paragraphs 1 through 13 of the Introduction to the Indictment above.

15. On or about January 28, 2014, within the Eastern District of Virginia and elsewhere, the defendant, ADAM C. MARKS, intentionally accessed a computer without authorization, and exceeded authorized access, and thereby obtained information from a protected computer used in interstate and foreign commerce, with the value of the information obtained exceeding $5,000, the defendant used the Internet to access the Salesforce.com portal and access Estes Forwarding Worldwide's Salesforce account and thereby obtained a file named "SalesForceData.zip" that contained confidential Estes Forwarding Worldwide customer information.

(In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(iii).)

COUNT TWO

(Knowingly and Intentionally Damaging a Protected Computer)

16. The Grand Jury realleges and incorporates the allegations of paragraphs 1 through 9 of the Introduction to the Indictment above.

17. From on or about December 23, 2013, to on or about December 24, 2013, within the Eastern District of Virginia and elsewhere, the defendant, ADAM C. MARKS, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and such conduct caused loss to Estes Forwarding Worldwide during the one-year period from December 23, 2013, to December 23, 2014, aggregating more than $5,000 in value.

(In violation of Title 18, United States Code, Section 1030(a)(5)(A).)

A TRUE BILL:

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office

FOREPERSON

DANA J. BOENTE
United States Attorney

By: _____
Brian R. Hood
Assistant United States Attorney